**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32 — A1

(11) International Publication Number: **WO 98/37663**

(43) International Publication Date: 27 August 1998 (27.08.98)

(21) International Application Number: PCT/SE98/00206

(22) International Filing Date: 5 February 1998 (05.02.98)

(30) Priority Data:
9700587-0 19 February 1997 (19.02.97) SE

(71) Applicant *(for all designated States except US)*: POSTGIROT BANK AB (publ) [SE/SE]; S-105 06 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: LEONARDI, Robert [SE/SE]; Gränsvägen 350, S-163 52 Spånga (SE).

(74) Agents: ÖRTENBLAD, Bertil et al.; Noréns Patentbyrå AB, P.O. Box 10198, S-100 55 Stockholm (SE).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: METHOD FOR AUTHORIZATION CHECK

(57) Abstract

Method for checking authorization incorporating a way to impart to a so-called smart card (SmartCard) an encryption key or equivalent key and including a way to cause a microprocessor, by means of the encryption key and at least one number, to perform a calculation whose result comprises a signature, and including a way to have said signature together with said number transferred to a system for which authorization is to be shown which includes a computer in which said encryption key is stored, said computer being programmed to carry out said calculation to obtain said signature and then to compare the latter signature with the first-mentioned signature.

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | |
|---|---|
| **AL** | Albania |
| **AM** | Armenia |
| **AT** | Austria |
| **AU** | Australia |
| **AZ** | Azerbaijan |
| **BA** | Bosnia and Herzegovina |
| **BB** | Barbados |
| **BE** | Belgium |
| **BF** | Burkina Faso |
| **BG** | Bulgaria |
| **BJ** | Benin |
| **BR** | Brazil |
| **BY** | Belarus |
| **CA** | Canada |
| **CF** | Central African Republic |
| **CG** | Congo |
| **CH** | Switzerland |
| **CI** | Côte d'Ivoire |
| **CM** | Cameroon |
| **CN** | China |
| **CU** | Cuba |
| **CZ** | Czech Republic |
| **DE** | Germany |
| **DK** | Denmark |
| **EE** | Estonia |
| **ES** | Spain |
| **FI** | Finland |
| **FR** | France |
| **GA** | Gabon |
| **GB** | United Kingdom |
| **GE** | Georgia |
| **GH** | Ghana |
| **GN** | Guinea |
| **GR** | Greece |
| **HU** | Hungary |
| **IE** | Ireland |
| **IL** | Israel |
| **IS** | Iceland |
| **IT** | Italy |
| **JP** | Japan |
| **KE** | Kenya |
| **KG** | Kyrgyzstan |
| **KP** | Democratic People's Republic of Korea |
| **KR** | Republic of Korea |
| **KZ** | Kazakstan |
| **LC** | Saint Lucia |
| **LI** | Liechtenstein |
| **LK** | Sri Lanka |
| **LR** | Liberia |
| **LS** | Lesotho |
| **LT** | Lithuania |
| **LU** | Luxembourg |
| **LV** | Latvia |
| **MC** | Monaco |
| **MD** | Republic of Moldova |
| **MG** | Madagascar |
| **MK** | The former Yugoslav Republic of Macedonia |
| **ML** | Mali |
| **MN** | Mongolia |
| **MR** | Mauritania |
| **MW** | Malawi |
| **MX** | Mexico |
| **NE** | Niger |
| **NL** | Netherlands |
| **NO** | Norway |
| **NZ** | New Zealand |
| **PL** | Poland |
| **PT** | Portugal |
| **RO** | Romania |
| **RU** | Russian Federation |
| **SD** | Sudan |
| **SE** | Sweden |
| **SG** | Singapore |
| **SI** | Slovenia |
| **SK** | Slovakia |
| **SN** | Senegal |
| **SZ** | Swaziland |
| **TD** | Chad |
| **TG** | Togo |
| **TJ** | Tajikistan |
| **TM** | Turkmenistan |
| **TR** | Turkey |
| **TT** | Trinidad and Tobago |
| **UA** | Ukraine |
| **UG** | Uganda |
| **US** | United States of America |
| **UZ** | Uzbekistan |
| **VN** | Viet Nam |
| **YU** | Yugoslavia |
| **ZW** | Zimbabwe |

# Method for authorization check

The present invention relates to a method for checking the authorization of a person, in his/her capacity as user of a system such as a payment system or a data system.

Systems now in existence are used to check the authorization of a person in connection with payment. One such system is used within the Swedish Postal Service for payments made via postgiro. In accordance with this system, the customer receives a so-called SmartCard and a card reader for it. An encryption key is stored on the SmartCard, and it can be read by a microprocessor on the SmartCard after a PIN code has been entered.

The said encryption key is stored not only on the SmartCard, but also at the Swedish Postal Service postgiro department where it is linked to a specific person.

When a payment is to be made, the user keys in the said PIN code, the number of the account to which the payment is to be sent and the amount in question. Herewith, the microprocessor performs a calculation based on the amount, the account number and the encryption key in accordance with the so-called DES (Data Encryption Standard) algorithm, wherewith a signature is generated by the said calculation. After this is done, the amount, the account number and the signature are transferred to the postgiro department in a suitable manner, via data, mail or fax for example.

The postgiro department receives the information and then performs the same calculation as set forth above and compares the result with the signature that was transferred. If the comparison results in a match, an authorized person, i.e. the holder of the SmartCard, is deemed to have ordered the transaction, wherewith the transaction is executed. The transaction is executed by transferring money from the postgiro

account of the SmartCard holder to the specified postgiro account.

This payment system is automatic, and it can be used to make payments at any time of day or night.

Obviously, it must be possible for the described system to be used by a person to show authorization for a system other than a postgiro or bank payment system. For example, it should be possible for a person to show authorization for a data system by entering his/her PIN code and two numbers other than an amount and account number, and then transferring them together with the signature to the data system. If the data system contains the encryption key the signature can be calculated, and if a match is found the person to whom the SmartCard has been issued can be deemed to be the person who entered the items of information and is therefore authorized.

However, a significant disadvantage of the described system is that the user must have access to a SmartCard and a special card reader in order make a payment.

The present invention solves this problem.

The present invention thus relates to a method for checking authorization that incorporates a way to impart to a so-called smart card (SmartCard) an encryption key or equivalent key, and incorporates a way to have a microprocessor, using the encryption key and at least one number, perform a calculation whose result comprises a signature, and incorporates a way to have the said signature together with the said number transferred to a system for which authorization is to be shown, wherewith such system includes a computer in which the said encryption key is stored, said computer being induced to perform the said calculation in order obtain the said signature, and incorporates a way for this latter signature to be compared by the computer with the previously mentioned signa-

ture, characterized in that the said smart card is a so-called SIM-card intended for mobile telephony and a memory in said SIM-card is, in a first step, provided with unique information containing a unique identity in order to communicate telephonically using a mobile telephone and in that, in a second step, the SIM-card memory is provided with said encryption key, and in that a system for which authorization is to be shown is provided with the same encryption key linked to an identity of the SIM-card, and in that in response to the entry of an appropriate code and at least the said number via the keyboard on the mobile telephone, a microprocessor on the said SIM-card is induced to perform the said calculation resulting in the said signature.

The present invention is not limited to any special field with regard to showing authorization. Instead, it is applicable for all kinds of systems such as payment systems, data systems, systems that check authorization before allowing entrance etc.

The description of the present invention that follows, however, is for a system that provides payment via postgiro.

The system is described in greater detail below, partially in connection with an example of an embodiment shown on the attached drawing, where:

- Fig. 1 shows the included hardware schematically.
- Fig. 2 shows a SIM-card.
- Fig. 3 shows a schematic view of a block diagram for which a function is described.
- Fig. 4 shows a schematic view of a block diagram for which another function is described.

Fig. 1 shows mobile telephone 1 of an appropriately known type which is intended for use in a GSM system or an equivalent telephone system where a so-called smart card

(SmartCard) is used together with the mobile telephone to form a usable communication unit. In the GSM system, the smart card is a SIM-card. The mobile telephone includes a keyboard 2 and a display 3.

Fig. 1 also shows a base station 4 for wireless communication with mobile telephone 1. In addition, a computer 5 is shown which belongs to the system with which the mobile telephone is to communicate.

Fig. 2 also shows a SIM-card 6 that incorporates a microprocessor 7 together with its memory.

The present invention relates to a method for checking authorization, wherewith a so-called smart card (SmartCard) is provided with an encryption key KEY or an equivalent key, and wherewith a microprocessor 7 is induced to perform, based on the encryption key and at least one number, a calculation whose result comprises a signature. The said number is entered into the microprocessor from a keyboard. The signature, together with the said number, is then transferred to a system for which authorization is to be shown which includes a computer 5 in which said encryption key has been stored. Computer 5 is induced to perform the said calculation to obtain the said signature. Computer 5 then compares this latter signature with the first-mentioned signature. If the two signatures match, authorization of the user is verified.

The method is thus based on the user having a SmartCard that incorporates an identity unique to the user and an encryption key. It is presupposed that only the user him/herself will use the SmartCard.

In accordance with the invention, the said smart card is a so-called SIM-card 6 intended for mobile telephony. In a first step, unique information that includes a unique identity (IMSI as set forth in the GSM standard) is entered into

memory 7 in said SIM-card 6 in such a way as to support telephonic communication using a mobile telephone. This appropriately takes place in the same as way as presently being used in the GSM system.

In a second step, the memory in SIM-card 6 is provided with the said encryption key. This memory can be the existing memory 7 or an extra memory. This is accomplished in a way that corresponds with the way the previously mentioned identity was entered, but it should preferably be carried out by the person who controls the system for which authorization is to be shown.

In accordance with the invention, the system for which authorization is to be shown is provided with the same encryption key linked to an identity for the SIM-card. Here, for example, the IMSI used for the SIM-card can serve as its identity ID. Alternatively, the encryption key in the said system can be linked to some other identity such as the user's telephone number, a customer number or a name. What is essential is that the system must later be able to retrieve the correct encryption key for a specified user.

The invention is further characterized in that when a suitable code is entered along with at least the said number via keyboard 2 on mobile telephone 1, a microprocessor on the said SIM-card is induced to perform the said calculation resulting in the said signature. The microprocessor can be the regular microprocessor that is normally incorporated into the SIM-card, but it can also be a separate microprocessor on the SIM-card. In the latter case, however, the separate microprocessor is linked to regular microprocessor 7 on the SIM-card.

The term "suitable code" means, for example, a code that is entered in order to put the mobile telephone in a mode in

which the microprocessor is induced to proceed with calculation of the signature.

Obviously, then, it suffices to have a mobile telephone and be able induce a microprocessor in a SIM-card to perform a calculation using an encryption key to obtain an electronic signature that can be transferred to a system for which authorization is sought, wherewith said system conducts an equivalent calculation, thereby determining whether or not authorization can be verified. As a result, no other equipment is needed to show authorization, as mentioned in the introduction.

After authorization has been verified in the aforesaid manner, the mobile telephone can be used to have the system perform services such as making payments in situations where the system is, for example, part of a postgiro system.

In accordance with a preferred embodiment, the said numbers comprise at least two numbers. This improves security significantly. When the invention is applied to perform payments made via postgiro for example one of the numbers can comprise the number of the account that is to receive a payment while the other can comprise the amount to be paid.

This is illustrated in Fig. 3 by numbers D1 and D2 which are sent to the microprocessor in the mobile telephone via the keyboard on the mobile telephone. When the numbers are entered, the microprocessor retrieves the encryption key KEY from memory MEM and conducts the aforesaid calculation which results in said signature SIG.

In accordance with a preferred embodiment, the signature calculated by the mobile telephone together with at least the said numbers is caused to be transferred via mobile telephone network 4 to said system.

In accordance with an alternative embodiment, the signature calculated by the mobile telephone together with at least the said numbers is caused to be transferred directly from the mobile telephone to said system via an interface between the mobile telephone and the system such as a computer 5 belonging to the system. The interface can comprise a cable 8 or an infrared link or some other suitable link.

In accordance with a preferred embodiment, the mobile telephone is caused to present the said signature on the mobile telephone display. In such case, the user can, for example, enter the said numbers and signature on a keyboard belonging to a computer that belongs to the system.

In accordance with a highly preferred embodiment, a special PIN code is assigned to the SIM-card in such a way that it can be used to enable the card for said calculation of the signature. This further enhances security since the user must a) know his/her PIN code to start the mobile telephone and b) know his/her PIN code to access and start the calculation process used to obtain the electronic signature.

To facilitate the making of correct payments for example and in accordance with a preferred embodiment, the mobile telephone is caused to present the said numbers on its display. An account number and an amount, for example, can be displayed before the signature is calculated.

When the signature has been calculated, data is thus transferred to the system. Herewith, as illustrated in Fig. 4, a user identity ID such as a telephone number, an IMSI or some other identity is always transferred. Signature SIG is also always transferred. Moreover, at least one number D1 or D2 is always transferred. If payments are involved, account number D1 and amount D2 are transferred. When this has happened, the system computer 5 retrieves the encryption key KEY that is linked to identity ID from a memory MEM and then calculates

the signature. When this is done, the computer compares the calculated signature with the signature SIG that was transferred from the mobile telephone. If the two signatures match, the user is deemed to have shown his/her authorization, whereupon payment 9 is made.

To further enhance security, a serial number can be included as one of the said numbers. If payments are involved, calculation is then performed on the basis of an account number, an amount and a serial number. The serial number can range from 00 to 99. When the first payment is made, serial number 00 is used, when the second payment is made serial number 01 is used and so forth. Correspondingly, the system increments the serial number by counting the number of payment transactions originating from the same user.

This means that each payment transaction generates a unique signature even if the same amount is paid to the same account number more than once.

It is obvious that the present invention, by using a mobile telephone, permits authorization to be checked vis-a-vis an arbitrary system and permits payments via postgiro or a bank at any time of day or night with excellent security and without requiring any extra equipment beyond a mobile telephone.

A number of different embodiments have been described above. However, it is obvious that the numbers on which calculation of the signature is based can be numbers other than those exemplified above. Moreover, information in addition to what is set forth above can be transferred from the mobile telephone to the system in order to verify authorization.

The present invention shall thus not be considered limited to the embodiments set forth above. Instead it can be varied within the scope set forth in the attached claims.

Claims

1. Method for checking authorization incorporating a way to impart to a so-called smart card (SmartCard) an encryption key or equivalent key and a way to induce a microprocessor, by means of the encryption key and at least one number, to carry out a calculation whose result comprises a signature, and a way to have said signature, together with said number, transferred to a system for which authorization is to be shown, where said system includes a computer in which said encryption key has been stored and to have said system perform said calculation whose result will comprise said signature, and a way to have the computer compare the latter signature with the first-mentioned signature characterized in that said smart card is a so-called SIM-card (6) intended for mobile telephony, and in that the memory (MEM) on said SIM-card is, in a first step, provided with unique information including a unique identity in order to communicate telephonically using a mobile telephone, and in that the memory on the SIM-card in a second step is provided with said encryption key (KEY), and in that a system for which authorization is to be shown is provided with the same encryption key (KEY) linked to an identity of SIM-card (6), and in that when a suitable code (PIN) is entered along with at least said number via the keyboard (2) on the mobile telephone (1), a microprocessor (7) on the said SIM-card is induced to perform the said calculation resulting in the said signature (SIG).

2. A method in accordance with claim 1, characterized in that the said number contains at least two numbers.

3. A method in accordance with claim 1 or 2, characterized in that the signature (SIG) calculated by the mobile telephone (1, 7) together with at least the said number is caused to be transferred to said system (5) via the mobile telephone network.

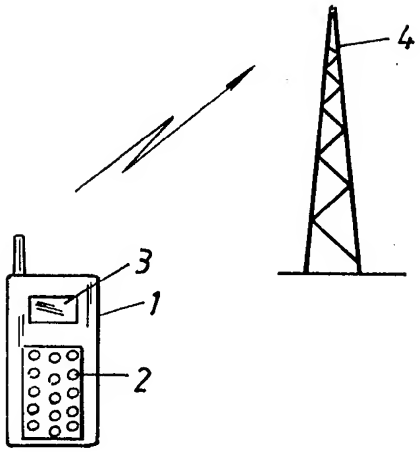
4. A method in accordance with claim 1 or 2, characterized in that the signature (SIG) calculated by the mobile telephone (1, 7) together with at least the said number is caused to be transferred directly from the mobile telephone (1) to said system (5) via an interface between the mobile telephone and the system, such as a computer belonging to the system.

5. A method in accordance with claim 1, 2, 3 or 4, characterized in that the mobile telephone (1) is caused to present said signature (SIG) on the display (3) on the mobile telephone.

6. A method in accordance with claim 1, 2, 3, 4 or 5, characterized in that a special PIN code is imparted to SIM-card (6) to enable it for the said calculation of signature.

7. A method in accordance with claim 1, 2, 3, 4, 5 or 6, characterized in that the mobile telephone (1) is caused to present the said number on its display (3).

Fig. 1



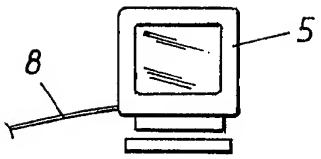




Fig. 2

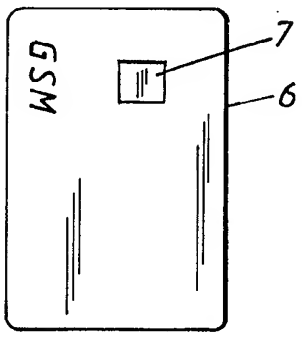



Fig. 3

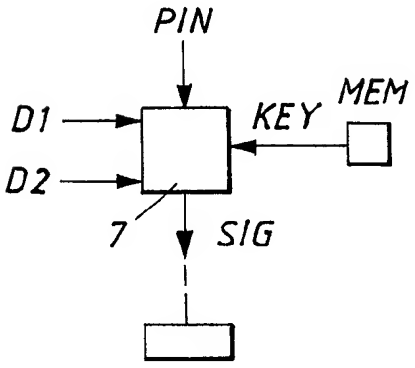
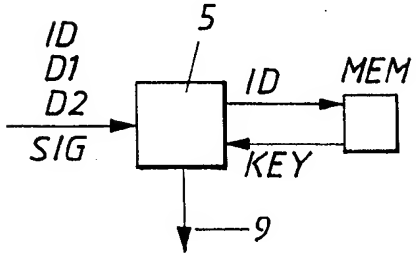



Fig. 4



# INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/00206

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 9605702 A2 (MOTOROLA INC.), 22 February 1996 (22.02.96), page 2, line 34 - page 3, line 31; page 12, line 19 - page 13, line 13 | 1-7 |
| A | EP 0708547 A2 (AT&T CORP.), 24 April 1996 (24.04.96), see the whole document | 1-7 |
| A | WO 9613814 A1 (VAZVAN, BEHRUZ), 9 May 1996 (09.05.96), see the whole document | 1-7 |
| A | WO 9411849 A1 (VATANEN, HARRI, TAPANI), 26 May 1994 (26.05.94), see the whole document | 1-7 |

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 22 July 1998 | 24 -07- 1998 |
| Name and mailing address of the ISA/<br>Swedish Patent Office<br>Box 5055, S-102 42 STOCKHOLM<br>Facsimile No. + 46 8 666 02 86 | Authorized officer<br>Rune Bengtsson<br>Telephone No. + 46 8 782 25 00 |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

30/06/98

International application No.
PCT/SE 98/00206

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9605702 A2 | 22/02/96 | BR 9506293 A | 11/11/97 |
| | | CA 2171017 A | 22/02/96 |
| | | EP 0721718 A | 17/07/96 |
| | | FI 961404 A | 28/03/96 |
| | | JP 9503895 T | 15/04/97 |
| | | US 5537474 A | 16/07/96 |
| | | US 5668875 A | 16/09/97 |
| EP 0708547 A2 | 24/04/96 | CA 2156206 A | 23/03/96 |
| | | JP 8096043 A | 12/04/96 |
| | | US 5608778 A | 04/03/97 |
| WO 9613814 A1 | 09/05/96 | EP 0739526 A | 30/10/96 |
| | | FI 100137 B | 00/00/00 |
| | | FI 945075 A | 29/04/96 |
| | | FI 962553 A | 25/11/97 |
| | | FI 962961 A | 28/08/96 |
| | | FI 971009 A | 26/04/97 |
| | | FI 971248 A | 26/04/97 |
| | | FI 971848 A | 30/04/97 |
| WO 9411849 A1 | 26/05/94 | AT 159602 T | 15/11/97 |
| | | DE 69314804 D,T | 12/02/98 |
| | | EP 0669031 A,B | 30/08/95 |
| | | SE 0669031 T3 | |
| | | ES 2107689 T | 01/12/97 |
| | | FI 925135 A | 12/05/94 |
| | | FI 934995 A | 12/05/94 |
| | | NO 951814 A | 09/05/95 |